

AO 93 (Rev. 11/13) Search and Seizure Warrant

## UNITED STATES DISTRICT COURT

for the  
Middle District of AlabamaIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)The residence and curtilage located at 26 E. Harris  
Drive, Fort Rucker, AL, including any outbuildings,  
vehicles, persons associated with address, and any  
computers or computer media - See Att's A1-A3 and B.

Case No.

1:19mj-133-SRW

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the \_\_\_\_\_ Middle \_\_\_\_\_ District of \_\_\_\_\_ Alabama  
(identify the person or describe the property to be searched and give its location):

See Attachments A1-A3 and B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachments A1-A3 and B.

YOU ARE COMMANDED to execute this warrant on or before May 10, 2019 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to Susan R. Walker  
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued:

April 30, 2019 9:43am

Judge's signature

City and state:

Montgomery, AL

Susan R. Walker, U.S. Magistrate Judge

Printed name and title

PENGAD 800-631-6888

GOVERNMENT  
EXHIBIT  
A

AO 106 (Rev. 04/10) Application for a Search Warrant

## UNITED STATES DISTRICT COURT

for the  
Middle District of Alabama

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)The residence and curtilage located at 26 E. Harris  
Drive, Fort Rucker, AL, including any outbuildings,  
vehicles, persons associated with address, and any  
computers or computer media - See Att's A1-A3 and B.

Case No.

1:19 mj 133-SRW

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachments A1-A3 and B.

located in the Middle District of Alabama, there is now concealed (identify the person or describe the property to be seized):

See Attachments A1-A3 and B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18, USC, §§ 2252A, (a)(1), (a) Transport, distribute, receive, and/or possess child pornography.  
(2), (a)(5)(B)

The application is based on these facts:

See attached Affidavit.

☒ Continued on the attached sheet.☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Neil J. D'Cunha, SA, USACIDC

Printed name and title

Sworn to before me and signed in my presence.

Date: April 29, 2019City and state: Montgomery, AL

Judge's signature

Susan R. Walker, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF ALABAMA  
SOUTHERN DIVISION

IN THE MATTER OF THE SEARCH OF )  
THE RESIDENCE AND CURTILAGE )  
LOCATED AT 26 E. HARRIS DRIVE, )  
FORT RUCKER, AL, INCLUDING ANY ) Case No. 1:19mj133SRW  
OUTBUILDINGS, VEHICLES, )  
PERSONS ASSOCIATED WITH ) **Filed Under Seal**  
ADDRESS, AND ANY COMPUTER(S) )  
OR COMPUTER MEDIA AS FURTHER )  
DESCRIBED IN ATTACHMENTS A1- )  
A3 & B. )

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT**

I, Neil J. D'Cunha, a Special Agent (SA) with the United States Army Criminal Investigation Command (USACIDC), being duly sworn, depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I have been a Special Agent with the USACIDC, since June 2014 and currently assigned to the Computer Crime Investigative Unit – Washington Metro Office (CCIU-WMO), and have been in this position since September 2018. During my tenure as a Special Agent, I have taken classes related to cyber-criminal activity and I am a Department of Defense certified Digital Forensic Examiner. I have also received training in investigations involving the sexual exploitation of children.

2. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A and I am authorized by law to request a search warrant. As part of my training and experience, I have reviewed images containing child pornography in a variety

of formats (such as digital still images and video images) and media (such as digital storage devices, the Internet, and printed images).

3. I am investigating the activities of an individual using an Internet Protocol (IP) address, **70.94.237.18**, registered to Christopher Dean Miers at the following address: 26 E. Harris Drive, Fort Rucker, AL 36362. As will be shown below, there is probable cause to believe that an individual(s) has used that IP address to transport, distribute, receive, and/or possess child pornography, in violation of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), (a)(5)(B).

4. I submit this application and affidavit in support of a search warrant authorizing a search of the residence and curtilage located at 26 E. Harris Drive, Fort Rucker, AL 36362, including any outbuildings, computers, or computer-related storage devices found thereon, as further described in **Attachment A1**; the search of a vehicle identified as a Black, Toyota Highlander bearing Alabama license plate 3122BB3 as further described in **Attachment A2**; and the person of Christopher Dean Miers as described in **Attachment A3** (hereinafter collectively referred to as the "PLACES TO BE SEARCHED"). I am also seeking authority to seize on and within the PLACES TO BE SEARCHED the items specified in **Attachment B** and subsequently search, that which may constitute evidence, fruits, and instrumentalities of the foregoing criminal violations.

5. The facts in this affidavit come from my own personal observations, my training and experience, and information obtained from other agents and witnesses. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and

instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(1), (a)(2), (a)(5)(B) are presently located in the PLACES TO BE SEARCHED.

### **CRIMINAL STATUTES**

6. This investigation concerns alleged violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors.

7. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping child pornography using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

8. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

9. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or accessing with intent to view any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped and transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

### **DEFINITIONS**

10. The following definitions apply to this Affidavit and Attachment B:

- a. The “American Registry for Internet Numbers” (ARIN), as the Regional Internet Registry for the United States. ARIN manages the distribution of Internet number resources and provides a free public database to search for assigned IP addresses.

- b. "BitTorrent," as a communications protocol of peer-to-peer file sharing ("P2P") which is used to distribute data and electronic files over the Internet.
- c. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- d. "Child Pornography," as used herein, includes the definition in Title 18, United States Code, Section 2256(8) any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct. Title 18, United States Code, Section 2256(8).
- e. "Cloud Storage," as used herein, means a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. Such hosting companies include Dropbox, iCloud, and Google Cloud Storage.
- f. "Computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such devices." For purposes of this search warrant, the term "computer" also encompasses computer software and data security devices.
- g. "Computer-related media," as used herein, encompasses all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data, including any data-processing devices (such as central processing units, internal drives, and fixed disks); peripheral storage devices (such as external hard drives, floppy diskettes, compact discs ("CDs"), digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), memory cards, Subscriber Identity Module ("SIM") cards, and USB thumb drives); peripheral input/output devices (such as modems, routers, keyboards, printers, scanners, copiers, monitors, web cams, digital cameras, iPods, cell phones, and video game consoles); as well as related equipment (such as cables and connectors).
- h. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- i. “Data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- j. “GUID” or “globally unique identifier,” as used herein, is a 128-bit (16 byte) number used by software programs (such as Shareaza and Limewire) to uniquely identify the location of a data object. The GUID is consistent across changes to the computer’s IP address, but it can be changed at will by the user.
- k. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.
- l. “Minor,” as used herein, means any person under the age of 18 years. Title 18, United States Code, Section 2256(1).
- m. “Records, documents, and materials,” as used herein, includes all information recorded in any form by any means, whether in handmade form (such as writings, drawings, or paintings), photographic form (such as developed film, print-outs, slides, negatives, or magazines), type-written form (such as print-outs, books, pamphlets, or other typed documents); audio/visual form (such as tape-recordings, videotapes, DVDs, or CDs), or electronic form (such as digital data files, file properties, computer logs, or computer settings).
- n. “Sexually explicit conduct,” as used herein, means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See Title 18, United States Code, Section 2256(2).

- o. “Visual depictions,” as used herein, include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See Title 18, United States Code, Section 2256(5).

**BACKGROUND ON CHILD PORNOGRAPHY AND  
THE USE OF ELECTRONIC STORAGE**

11. I have had both training and experience in the investigation of internet related crimes. Based on my training, experience, and knowledge, I know the following:

- a. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- b. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where an individual uses online storage, however, law enforcement can find evidence of child pornography on the user’s computer, smartphone or external media in most cases.
- c. As is the case with most digital technology, communications by way of email can be saved in their inbox or stored on a computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files) or unintentional. Digital information such as the traces of the path of an electronic communication may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information exists indefinitely until overwritten by other data.
- d. Individuals who use email to obtain child pornography often have saved contacts or communication via that email account with others who may be sharing, receiving or advertising child pornography.

12. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had

discussions, I have learned that individuals who use the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

- a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.
- e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and

materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

- f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer-to-Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who use these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.
- g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.
- h. In my training and experience, persons who repeatedly use a Peer-to-Peer network to share child pornography, particularly over a period of time rather than on a single occasion, tend to save, collect and make these images available for re-sharing on the Peer-to-Peer network that they use. As set forth in the Probable Cause section below, the subject of this search warrant, an individual using the Bittorrent P2P file sharing network, was observed sharing child pornography twice over the past three months using the same IP address and the same Peer-to-Peer network. As stated above, this is consistent with the behavior of persons who access and collect child pornography.

#### **PEER-TO-PEER (P2P) FILE SHARING**

13. Peer-to-peer (P2P) file sharing computer software programs are a standard way to transfer files from one computer system to another while connected to a network, usually the Internet. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to connect directly to each other to share files. Many P2P file sharing networks are designed to allow users to download files and frequently provide enhanced

capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Typically, settings within these programs control sharing thresholds.

14. I know from my training and experience that P2P file sharing networks are frequently used to trade digital files of child pornography. These files include both image and video files.

15. During the default installation of most P2P software applications, settings are established which configure the host computer to share files. Depending upon the software application used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed. Typically, there are settings that allow the user to establish the location of one or more directories or folders whose contents (files) are made available for distribution to other network users and to control (a) whether or not files are made available for distribution to other network users; (b) whether or not other network users can obtain a list of the files being shared by the host computer; and (c) whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.

16. There is a feature inherent in all P2P programs that allows for requesting a shared file listing directly from a computer. P2P investigators have received training and have used the features built into the P2P Client software programs to request a file listing of "shared files" from various computers during undercover P2P operations. The command used is commonly called a "browse." This command allows the computer host (a host is a term used to describe a computer connected to the Internet) making the request to "browse" or look through a listing of files by

name, file type, quality and SHA-1 values that the user on the other end has specifically placed or downloaded into a specific folder for sharing with others on the P2P Network. A browse command is sometimes available to any and all users on the different file sharing Networks and is part of the commonality in most file sharing programs, including Limewire, Shareaza, and Lemonwire. Users can and do share or have files in their shared folder available for searches and downloads on the file sharing Networks. Users can also disallow "browsing" of their shared files. Anyone who routinely uses and downloads files would know they are downloading from other users who have allowed file sharing on their computer. The sharing concept is the whole concept and reason for a user installing a P2P client or software. Conversely, they would also know that certain files on their computer are available for download unless they intentionally change the configuration of the client software to disallow those downloads and browsing commands from others on the network.

17. Files located in a network user's shared directory are processed by the client software. As part of this processing, a SHA1 hash value is computed for each file in the user's shared directory. SHA1 or Secure Hash Algorithm Version 1 is a file encryption method which may be used to produce a unique digital signature of a file. It is computationally infeasible ( $2^{160}$ ) to find two different files that produce the same SHA1 value. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard. A file processed by this SHA1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide a certainty exceeding 99.99 percent that two or more

files with the same SHA1 signature are identical copies of the same file regardless of their file names.

18. Some P2P networks use SHA1 values to improve network efficiency. Users may receive a selected file from numerous sources by accepting segments of the file from multiple peers and then reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. The network uses SHA1 values to ensure exact copies of the same file are used during this process. It is possible to compare the SHA1 signatures of files being shared on the network to previously identified SHA1 signatures of any file, including child pornography, to determine if the contents of the two files are identical.

19. A P2P file transfer is assisted by reference to an IP address. The IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers. IP addresses can also assist law enforcement in finding a particular computer on the Internet. Typically, an IP address will lead the law enforcement officer to a particular Internet service company, and that company can then identify the account that used the IP address to access the Internet on a given date and time.

20. By receiving either a file list or portions of a download from a specific IP address, the investigator can conclude that a computer connected to that particular IP address is using a P2P software application to receive, distribute, and/or possess specific and known visual depictions of child pornography.

21. Even though P2P networks link together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user without that user's knowledge. The software is designed only to allow files that have been selected to be

downloaded. One does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active participation.

22. A person that includes child pornography files in his/her "shared" folder is making those child pornography files available for other network users to download. Therefore, the hosting of child pornography in this way constitutes the promotion and distribution of child pornography in violation of federal law.

23. This investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of the officers involved in this effort are using the technology and methods described herein. This methodology has led to the issuance and execution of search warrants around the country resulting in many seizures of child pornography and arrests for possession and distribution.

#### **BITTORRENT PEER-TO-PEER FILE SHARING**

24. BitTorrent, one type of P2P software, sets up its searches by keywords typically on torrent websites. BitTorrent programs are typically free to download and used for the exchange of files between computer users.

25. The results of a keyword search are displayed to the user. The website does not contain the files being shared only file referred to as a "torrent." The user then selects a .torrent file(s) from the results for download. This .torrent file contains instructions on how a user can download the file(s) referenced in the Torrent. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the actual files (not the torrent file but the actual files referenced in the .torrent file using any BitTorrent client.)

26. For example, a person interested in obtaining child pornographic images would open the BitTorrent website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user selects a .torrent from the results displayed the file(s) he/she wants to download. Once the .torrent file is downloaded, it is used by a BitTorrent program which the user had previously installed. The .torrent file is the set of instructions the program needs to find the files referenced in the .torrent file. The file(s) is downloaded directly from the computer or computers sharing the file. The downloaded file(s) is stored in the area previously designated by the user and/or the software. The downloaded file will remain until moved or deleted.

27. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file.

28. The computer running the file sharing application, in this case a BitTorrent application, has an IP address assigned to it while it is on the internet. BitTorrent users are able to see the IP address of any computer system sharing files to them or receiving files from them. Investigators log the IP address which has sent them files or information regarding files being shared. Investigators can then search public records (ARIN) that are available on the internet to determine the internet service provider who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the internet service provider.

**SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

29. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computers and computer-related media, to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices (such as hard disks, CDs, and USB thumb drives) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order and with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on-site or even within the period specified for execution of the search warrant.
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computers and computer-related media available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or even normal activities of an operating system), the controlled environment of a laboratory is ideal for a complete and accurate analysis.

30. In finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For instance, based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that when a computer has more than one user, files can contain information indicating the dates and times that they were created,

as well as the sequence in which they were created. For example, by reviewing the Index.dat file (a system file that keeps track of historical activity conducted in the Internet Explorer application), it can be determined whether a user accessed other information close in time to the file creation dates, times and sequences so as to establish user identity and exclude others from computer usage during times related to the criminal activity.

### **PROBABLE CAUSE**

31. On February 5, 2019, SA Vincent Olman, CCIU-WMO, identified a device assigned the Internet protocol (IP) address 70.94.237.18 (hereinafter "SUSPECT IP"), connected to the BitTorrent Network and transmitting files depicting child pornography. The SUSPECT IP address was geo-located to Fort Rucker, AL, via Maxmind geo-location services.

32. On February 5, 2019, SA Olman downloaded two files from the SUSPECT IP. These files were reviewed and described as follows:<sup>1</sup>

- a. [REDACTED]: This video is 12 minutes and 46 seconds in length, shown in color and with sound. The video depicts two Caucasian female minors in an indoor setting on a bed. In the bottom left appears the wording, "VIDEO EDIT BY MUMMY." Both minors are initially wearing underwear and towels on their heads. The minors appear to play on the bed, undressing each other until both are nude. The minors continue to play while the camera zooms-in and focuses on their genitals several times.
- b. [REDACTED]: This video is 6 minutes and 18 seconds in length, shown in color and with sound. The video depicts two Caucasian female minors in an indoor setting. In the bottom right appears the wording, "VIDEO EDIT BY MUMMY." Both minors are initially wearing leotards and one also has on a skirt. The minors appear to play on a couch, undressing each other until one is nude and the other is only wearing the skirt. The minors continue to play, and at several times, they spread their legs and expose their genitals to the camera.

---

<sup>1</sup> A copy of the described child pornography was made available for review by the Magistrate Judge and will be kept in a secure location by the affiant.

33. A search of the SUSPECT IP in the ARIN database revealed it was registered to Charter Communications LLC, 400 Atlantic Street, Stamford, CT 06901.

34. Subpoena results received from Charter Communications LLC, established the SUSPECT IP was assigned to Christopher Dean Miers, 26 E. Harris Drive, Fort Rucker, AL 36362, during the time the contraband files were downloaded by USACIDC.

35. Department of Defense database records indicate that Christopher Dean Miers is an active duty U.S. Marine Recruiter assigned to Montgomery, AL, and resides at 26 E. Harris Drive, Fort Rucker, AL 36362. Database records also indicate other possible occupants at this residence to be Mrs. Christina N. Miers (Spouse of Christopher Dean Miers), and Christopher Dean Miers' seven year old and four year old dependent children.

36. Fort Rucker CID Office confirmed that Christopher Dean Miers resides at 26 E. Harris Drive, Fort Rucker, AL 36362. Fort Rucker CID Office also observed Christopher Dean Miers owns and operates a black Toyota Highlander bearing Alabama license plate 3122BB3, which is registered to his residence, 26 E. Harris Drive, Fort Rucker, AL 36362.

37. Between April 20, 2019 and April 21, 2019, the SUSPECT IP continued to share child pornography via the BitTorrent network. On April 22, 2019, SA Olman downloaded nine files from the SUSPECT IP. Five of the nine files contained suspected child pornography. The following is a brief description of two of the downloaded files:<sup>2</sup>

- a. [REDACTED]: This video is 13 minutes and 5 seconds in length, shown in color and with sound. The video depicts two Caucasian female minors in an indoor setting. Both minors are partially clothed and appear to play, while undressing each other until both are nude. The minors continue to play while the camera zooms-in and focuses on their genitals several times.

---

<sup>2</sup> A copy of the described child pornography was made available for review by the Magistrate Judge and will be kept in a secure location by the affiant.

- b. [REDACTED] This video is 10 minutes and 49 seconds in length, shown in color and with sound. The video depicts two Caucasian female minors in an indoor setting sitting on a bed. Both minors are initially fully clothed and appear to be repeatedly jumping on the bed. The minors then undress until they are fully nude, while the camera zooms-in and focuses on their genitals several times.

### **FORENSIC ANALYSIS**

38. As described in Attachment B, this application seeks permission to search and seize records that might be found in the PLACES TO BE SEARCHED described in Attachments A1, A2, and A3 in whatever form they are found. I submit that if a computer or electronic medium is found in these locations, there is probable cause to believe those records will be stored in that computer or electronic medium, for at least the following reasons:

39. Based on knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

40. There is probable cause to believe that things that were once stored on the device(s) may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
- e. I know from training and experience that child pornographers generally prefer to store images of child pornography in electronic form as computer files. The computer's ability to store images in digital form makes a computer an ideal repository for pornography. A small portable disk or computer hard drive can contain many child pornography images. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection. In my training and experience, individuals who view child pornography typically maintain their collections for many years and keep and collect items containing child pornography over long periods of time; in fact, they rarely dispose of their sexually explicit materials.
- f. In this case, the affidavit requests permission to search and seize images of child pornography, including those that may be stored on a computer. These things constitute both evidence of crime and contraband. This affidavit also requests permission to seize the computer hardware and electronic media that may contain those things if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. In this case, computer hardware that was used to store child pornography is a container for evidence, a container for contraband, and also itself an instrumentality of the crime under investigation.

41. Based upon my knowledge, training and experience, I know that searching for information stored in computers often requires agents to seize most or all electronic storage devices to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is often necessary to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to

properly examine those storage devices in a laboratory setting, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the laboratory setting. This is true because of the following:

- a. The volume of evidence. Computer storage devices (like hard disks or CD-ROMs) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.
- b. Technical requirements. Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis.

42. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. Forensic evidence on a device can indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

- a. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- b. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- c. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

43. In light of these concerns, I hereby request permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

44. Searching computer systems for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, CCIU-WMO intends to use

whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

### **BIOMETRICS**

45. The search warrant I am applying for would permit law enforcement to compel the use of Christopher Dean Miers' biometric features. I seek this authority based on the following:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to use.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.
- d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During

the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. Further based on my training and experience, law enforcement personnel may not be able to fully execute the search authorized by this search warrant and thereby access the data contained within such device(s) without the use of biometric features.
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.
- h. In my training and experience, the person(s) who is or are in possession of a device or has the device among his or her belongings or at his or her premises at the time the device is found is likely to be a user of the device.
- i. Due to the foregoing, if law enforcement personnel encounter device(s) that is or are subject to seizure pursuant to this search warrant and may be

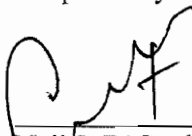
unlocked using one of the aforementioned biometric features, the search warrant I am applying for would permit law enforcement personnel, acting as soon as reasonably practicable, to compel the following: (1) press or swipe the fingers (including thumbs) of Christopher Dean Miers to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face of Christopher Dean Miers and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of Christopher Dean Miers and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this search warrant.

### CONCLUSION

46. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

47. Based upon the foregoing information, I have probable cause to believe that contraband, and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A, (a)(1), (a)(2), (a)(5)(B), as set forth herein and in Attachment B, are currently contained in the PLACES TO BE SEARCHED more fully described in Attachments A1, A2, and A3. I therefore respectfully request that a search warrant be issued authorizing a search of the PLACES TO BE SEARCHED for the items described above and in Attachment B and authorizing the seizure and examination of any such items found therein.

Respectfully submitted,



Neil J. D'Cunha  
Special Agent, USACIDC

Subscribed to and sworn before me this  
30 ~~th~~<sup>th</sup> day of April, 2019.  
SPW



---

SUSAN R. WALKER  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A1**  
**DESCRIPTION OF THE PREMISES TO BE SEARCHED**

26 E. Harris Drive, Fort Rucker, AL 36362, is a single story, single family home with a one car garage. The exterior is yellow, white, tan and green siding. The number "26" is displayed next to the front door along the support pillar. The PLACES TO BE SEARCHED includes the entire lot, any structures on the lot, and any automobiles present on the property. The photograph below depicts the residence.



ATTACHMENT A2

DESCRIPTION OF VEHICLE TO BE SEARCHED

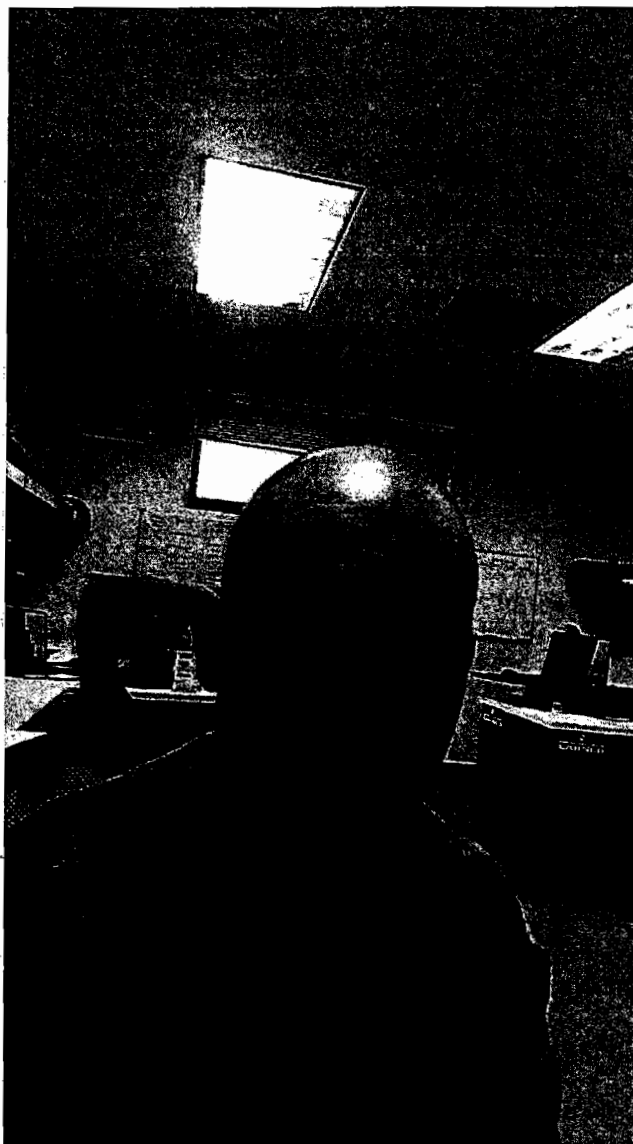
Black, 2014 Toyota Highlander bearing Alabama license plate 3122BB3



**ATTACHMENT A3**

**DESCRIPTION OF PERSON TO BE SEARCHED**

Christopher Dean Miers, DOB: XX/XX/1987, SSN: XXX-XX-5519, who is a white male, with black hair, HT 5'09", WT 180 lbs. A photograph of Christopher Dean Miers is shown below.



**ATTACHMENT B**

**DESCRIPTION OF PROPERTY TO BE SEIZED**

Any and all records relating to violations of Title 18, United States Code, Section 2252A, Transportation, Receipt, Distribution and Possession of Child Pornography, including:

1. Any and all computers, mobile devices, or storage media used as a means to commit the violations described above.
2. Any and all records, documents, and materials pertaining to any visual depiction of a minor engaging in sexually explicit conduct, child pornography, child erotica, a sexual interest in children, or sexual activity involving children.
3. Any and all records, documents, and materials pertaining to any minor who is, or appears to be, the subject of any visual depiction of a minor engaging in sexually explicit conduct, child pornography, child erotica, a sexual interest in children, or sexual activity involving children.
4. Any and all records, documents, and materials evidencing possession, use, or ownership of any of the premises to be searched or property to be seized.
5. Any and all records, documents, and materials that concern any Internet accounts or any Internet-related activity.
6. Any and all software that may be used to create, receive, distribute, store, modify, conceal, or destroy any of the evidence sought.
7. For any computer, mobile device or storage medium whose seizure is authorized by this warrant, and any image of such computer or storage medium (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this search and seizure warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved

usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;
- h. evidence of the times the computer was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the computer;
- j. documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;
- k. records of or information about Internet Protocol addresses used by the computer;
- l. records of or information about the computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this attachment.

8. Routers, modems, and network equipment used to connect computers to the Internet.

9. As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

10. The term “computer,” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

11. The term “storage medium,” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, DVDs, and other magnetic, electronic, or optical media.

12. During the execution of the search of the PLACES TO BE SEARCHED described in Attachments A1, A2 and A3, if law enforcement personnel encounter device(s) that is or are subject to seizure pursuant to this search warrant and may be unlocked using one of the biometric features referenced in paragraph 45 of the Affidavit in Support of An Application for A Search and Seizure Warrant, such law enforcement personnel are authorized, acting as soon as reasonably practicable, to compel Christopher Dean Miers to (1) press or swipe his fingers (including thumbs) to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face of the Christopher Dean Miers and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of the Christopher Dean Miers and activate the iris recognition feature, for the purpose of

attempting to unlock the device(s) in order to search the contents as authorized by this search warrant.

IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF ALABAMA  
SOUTHERN DIVISION


IN THE MATTER OF THE SEARCH OF )  
THE RESIDENCE AND CURTILAGE )  
LOCATED AT 26 E. HARRIS DRIVE, )  
FORT RUCKER, AL, INCLUDING ANY ) Case No. 1:19mj 133-SRW  
OUTBUILDINGS, VEHICLES, )  
PERSONS ASSOCIATED WITH ) **Filed Under Seal**  
ADDRESS, AND ANY COMPUTER(S) )  
OR COMPUTER MEDIA AS FURTHER )  
DESCRIBED IN ATTACHMENTS A1- )  
A3 & B. )

**MOTION TO SEAL**

The United States of America, by and through United States Louis V. Franklin, Sr., herein applies for an Order sealing the above-captioned case, and all filings in this matter, except that the Government requests that working copies of any pleadings may be made available, as necessary, to the United States Attorney's Office, the United States Army Criminal Investigation Command (USACIDC), and any other law enforcement agency designated by the United States Attorney's Office. As grounds for this Motion, the Government states that there is an ongoing investigation in this case, and allowing these documents to be accessible to the public would compromise the investigation and risk the safety of the law enforcement officers involved.

Respectfully submitted this 30<sup>th</sup> day of April, 2019.

FOR THE UNITED STATES ATTORNEY  
LOUIS V. FRANKLIN, SR.

  
\_\_\_\_\_  
Russell T. Duraski  
Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF ALABAMA  
SOUTHERN DIVISION

IN THE MATTER OF THE SEARCH OF )  
THE RESIDENCE AND CURTILAGE )  
LOCATED AT 26 E. HARRIS DRIVE, )  
FORT RUCKER, AL, INCLUDING ANY ) Case No. 1:19mj133-SRW  
OUTBUILDINGS, VEHICLES, )  
PERSONS ASSOCIATED WITH ) **Filed Under Seal**  
ADDRESS, AND ANY COMPUTER(S) )  
OR COMPUTER MEDIA AS FURTHER )  
DESCRIBED IN ATTACHMENTS A1- )  
A3 & B. )

**ORDER TO SEAL**

The Court, having considered the Government's Motion to Seal in the above-captioned case, and for good cause shown, hereby ORDERS that the above-captioned case, and all filings in this matter, are hereby sealed until further Order of the Court, except that working copies of any pleadings may be made available to the United States Attorney's Office, the United States Army Criminal Investigation Command (USACIDC), and any other law enforcement agency designated by the United States Attorney's Office.

DONE and ORDERED this 30th day of April, 2019.



SUSAN R. WALKER  
UNITED STATES MAGISTRATE JUDGE